โดนจนได้ไวรัส

บุญเลิศ เอี่ยมทัศนา

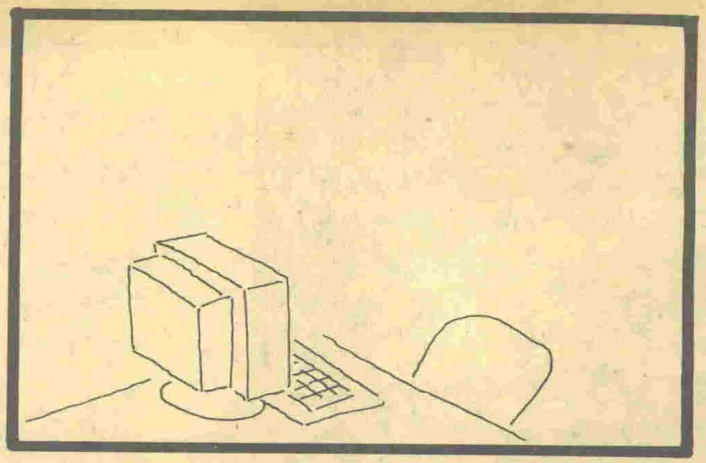
เพื่อไม่ให้น้อยหน้าใคร เครื่องไมโครคอมพิวเตอร์ในที่ทำงานของผมก็โดนไวรัสเล่นงานจนได้ เป็นพันธุ์ที่กำลังฮิตติดอันดับอยู่ในขณะนี้เสียด้วยคือ Israeli ที่เรียกขานกันว่า sUMsDoS ทำให้เสียงานไปหลายวัน ผมจึงขอนำเรื่องราวของเจ้าไวรัสตัวนี้มาเล่าสู่กันฟัง เผื่อใครประสบปัญหาแบบเดียวกับผมจะได้หาทางแก้ไขได้ทันท่วงที

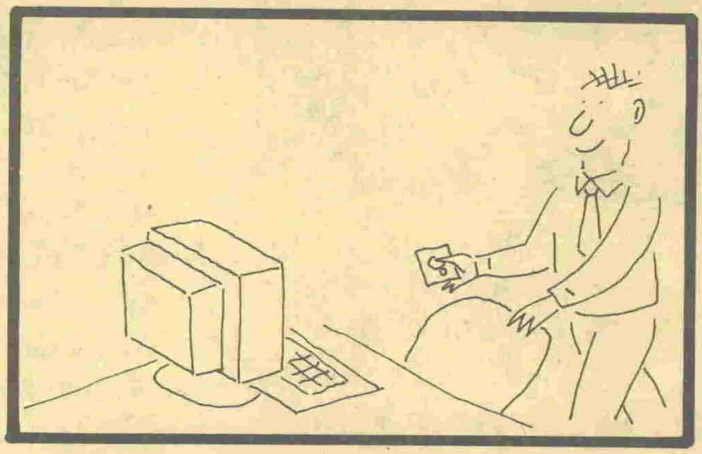
การทำงาน

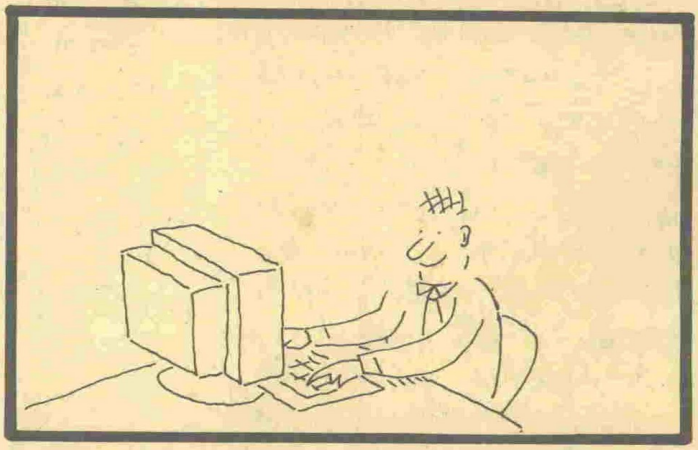
ผมคิดว่าการที่จะทราบถึงวิธีป้องกันมันได้อย่างไร ควรจะรู้การทำงานของมันก่อน คือ เริ่มแรกทีเดียวก็ต้องมีมนุษย์สติวิปลาสสร้างมันขึ้นมาโดยให้เกาะติดกับไฟล์ .EXE หรือ .COM ก็ได้ของโปรแกรมใดโปรแกรมหนึ่ง เมื่อมีผู้นำไปใช้งานหรือรันโปรแกรมนี้ เจ้า sUMsDOS ก็จะฝังตัวอยู่ในหน่วยความจำ พร้อมกับขยายตัวของมันในไฟล์ของโปรแกรมเดิมนี้อีก 1808 ไบต์สำหรับไฟล์ .EXE

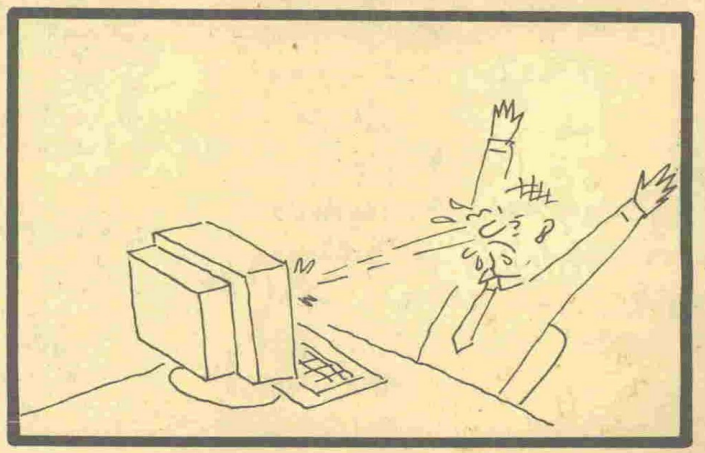
ถึงแม้ขณะนี้ไฟล์อื่นในทุกไดรฟ์ยังคงปลอดภัย แต่เมื่อจบโปรแกรมนี้แล้วรันโปรแกรมอื่น ไม่ว่าจะอยู่ในไดรฟ์ใดรวมทั้งในฮาร์ดดิสก์ซึ่งส่วนมากอยู่ในไดรฟ์ C ด้วย เจ้า sUMsDoS จะโหลดโปรแกรมใหม่นี้ไว้ในหน่วยความจำ ดำเนินกรรมวิธีเกาะติดกับโปรแกรมที่เรียกมาใหม่แล้วเก็บลงดิสก์ ทำให้ขนาดของไฟล์โตขึ้นอีก 1808 ไบต์ และจากนั้นโปรแกรมใหม่นี้ก็จะกลายเป็นตัวแพร่เชื้อต่อไป พร้อมทั้งทำให้โปรแกรมขยายตัวขึ้น 1808 ไบต์ทุกครั้งที่รัน

ถึงไวรัสจะมีพิษสงร้ายกาจขนาดไหน
ใช่ว่าหมดหนทางพิชิตมันเอาซะเลย
เพราะธรรมะย่อมชนะอธรรมเสมอ









ดู ๆ ก็ไม่น่าร้ายแรงนักหรอกครับ เพราะจะติดเชื้อเฉพาะไฟล์ .EXE กับ .COM (มีผู้กล่าวว่าติดกับไฟล์ที่เป็น Overlay ด้วย) ซึ่งรันขณะที่มี sUMsDoS ฝังตัวอยู่เท่านั้น แต่ไฟล์เหล่านี้ก็จะขยายตัวขึ้นเรื่อย ๆ และแพร่เชื้อต่อไป จนกระทั่งไม่สามารถรันโปรแกรมเหล่านั้นได้

เหตุการณ์ที่แย่ยิ่งกว่านี้ก็คือ มีผู้กล่าวว่าถ้ารันโปรแกรมเหล่านี้ในวันศุกร์ที่ 13 (เช่น ศุกร์ที่ 13 ตุลาคม 2532) มันจะลบโปรแกรมนั้น ๆ และอาจลามปามไปถึงไดเรคทอรีด้วย จึงไม่ควรให้มันแทรกอยู่ในระบบคอมพิวเตอร์ของคุณโดยเฉพาะเครื่องที่ติดตั้งฮาร์ดดิสก์

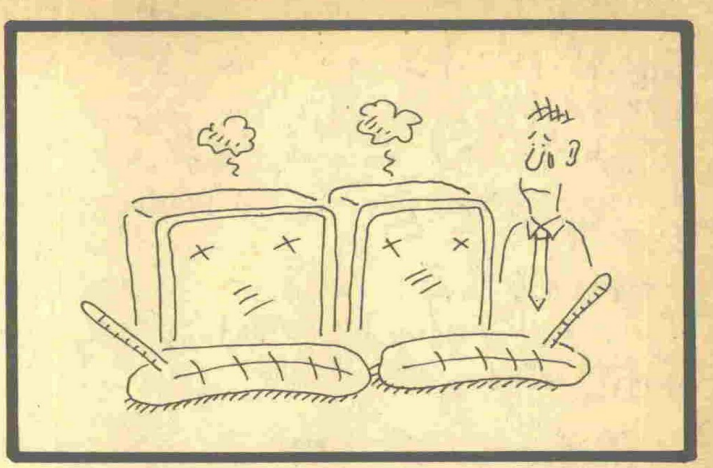
มันมาจากไหน

คำตอบง่าย ๆ คือมาจากไฟล์ .EXE หรือ .COM ที่มีไวรัสชนิดนี้เกาะติดอยู่ แต่เหตุการณ์ที่เกิดในที่ทำงานของผมชวนให้คิดว่ามาจากซอฟต์แวร์ต่างประเทศที่ป้องกันการก๊อบปี้ในแบบไวรัสพร้อมลายนิ้วมือ

เป็นธรรมดาครับสำหรับการรันโปรแกรมที่อ่าน/เขียนกับดิสก์ตลอดเวลา เรามักจะไม่ใช้แผ่นต้นฉบับ ผู้ที่ทดลองใช้ซอฟต์แวร์นี้จึงใช้ DISKCOPY มาใช้งานแทน มันกลับทำงานได้บ้างไม่ได้บ้างอยู่ร่วมสัปดาห์จนพบไวรัส แต่ก็จะปักใจเชื่อนักไม่ได้ เพราะยังมีผู้อื่นมาใช้เครื่องด้วย ผมจึงสั่งซอฟต์แวร์ตัวนี้มาใหม่ เพื่อพิสูจน์เรื่องนี้ให้เห็นดำเห็นแดง หากได้ผลประการใดจะเรียนให้ทราบต่อไป (แต่คงอีกหลายเดือนครับ)

เครื่องไม้เครื่องมือ

ก่อนที่จะกล่าวต่อไปผมคิดว่าควรจะแนะนำเครื่องไม้เครื่องมือที่เอามาใช้ต่อกรกับมันก่อน โดยจะกล่าวจากกว้างไปจนถึงที่เฉพาะเจาะจง ดังนี้



PIG

โปรแกรมนี้ผมเขียนขึ้นเองดังแสดงในรูปที่ 1 เพื่อจะใช้เป็นหนูตะเภา (guinea-pig) ในการตรวจสอบว่ามีไวรัสพันธุ์นี้แอบซ่อน (ฝังตัว) อยู่ในหน่วยความจำหรือไม่ โดยอาศัยหลักว่าเจ้าไวรัสนี้จะทำให้โปรแกรมโตขึ้น ดังนั้นเมื่อรัน PIG มันจะตรวจตัวเองว่าโตเท่าเดิมหรือไม่ ถ้าเท่าเดิมก็จะบอกว่าเรียบร้อย ถ้าไม่เท่าเดิม (ถูกไวรัสเกาะติด) ก็จะบอกว่ามีไวรัสซึ่งเราจะต้องลบมันทิ้งด้วย จึงได้ชื่อว่าเป็นหนูตะเภา

PC Tools หรือ Norton Utility

ใช้สำหรับตรวจหาคำว่า sUMsDoS ในไฟล์หรือในดิสก์ คำนี้จะปรากฏอยู่ในไฟล์ที่เจ้าไวรัสตัวนี้เกาะติดอยู่ และจะพบหลายแห่งด้วยเพราะมันจะประทับชื่อมันทุกครั้งที่มันเกาะหรือขยายตัว แต่การรันโปรแกรมทั้งสองนี้จะต้องรันก่อนที่จะมีไวรัสฝังตัวอยู่หรือใช้ดิสก์ที่ปิด Write Protected ไม่เช่นนั้น ตัวมันเองก็จะโดนไวรัสเกาะติดด้วย

KILL

โปรแกรมนี้ใช้สำหรับไวรัสพันธุ์นี้โดยเฉพาะ แต่ชื่ออาจทำให้

รูปที่ 1 โปรแกรมทดสอบไวรัสแบบ Israeli

ในการป้อนโปรแกรมให้เปลี่ยนตัวเลข 2928 เป็น 1000 แล้วคอมพายล์เป็นไฟล์ PIG.EXE เมื่อทดลองรันมันจะแสดงว่ามีไวรัส ให้เราเรียกออกไปที่ DOS จดขนาดของไฟล์ PIG.EXE ไว้ นำมาป้อนแทน 1000 (เพราะการป้อนโปรแกรมแต่ละครั้งอาจได้ขนาดของไฟล์ไม่เท่ากัน) จากนั้นจึงค่อยคอมพายล์เป็นไฟล์ .EXE ใหม่ เมื่อทดลองรันเครื่องจะต้องตอบว่าไม่มีไวรัส. *(หมายเหตุ : ความจริงสามารถเทียบ FileSize ได้โดยตรง)*

```
program  Pig;
var   size : Word;
      fi   : File;
begin
  Assign(fi,'PIG.EXE');
  {$I-}  Reset(fi,1);  {$I+}
  if  IOresult <> 0  then  Halt(1);
  size := FileSize(fi);
  if  size = 2928  then
    begin  WriteLn('No VIRUS in memory');
           WriteLn('   I am healthy')  end
  else
    begin  WriteLn(^G^G^G,'*** VIRUS IS DETECED IN MEMORY ***');
           WriteLn('          I am also sick');  end;
end.
```

ฉงน ความจริงโปรแกรมนี้ไม่ได้ฆ่าไวรัสครับ เป็นโปรแกรมที่เมื่อรันแล้วจะคงผลอยู่ในหน่วยความจำ RAM ป้องกันไม่ให้ไวรัสออกมาอาละวาดจนกว่าจะปิดเครื่อง ในหน่วยงานผมใช้อยู่หลายวันก่อนที่จะฟอร์แมตฮาร์ดดิสค์ใหม่ ทำให้ไม่มีปัญหาจากไวรัสพันธุ์นี้ซึ่งมีอยู่หลายสิบตัวในฮาร์ดดิสค์

PURE

โปรแกรมที่ทำหน้าที่กำจัดไวรัสพันธุ์นี้ออกไปจากไฟล์ ผมเคยทดลองใช้ดูเท่านั้น แต่ไม่ได้ใช้งานจริง เพราะใช้วิธีฟอร์แมตดิสค์ใหม่หมด

การป้องกัน

สำหรับปัญหาเรื่องของไวรัสแล้วผมมีความเห็นว่า ควรหามาตรการป้องกันเป็นดีที่สุด และผมขอกล่าวเน้นหนักเกี่ยวกับเครื่องที่ติดตั้งฮาร์ดดิสค์ เพราะมีปัญหามากกว่าใครเพื่อน โดย ขอแยกเป็นข้อ ๆ ดังนี้

- ถ้าคุณคิดว่าเครื่องของคุณปราศจากไวรัสและไม่ติดต่อกับใครเลย (ไม่ว่าทางสายหรือทางฟลอปปี้ดิสค์) ก็ไม่ต้องดำเนินการใด แต่ถ้าเป็นเครื่องที่ใช้ร่วมกันหลายคน โดยเฉพาะในสถาบันการศึกษา ขอให้รันโปรแกรม KILL ตั้งแต่บูตเครื่อง โดยใส่ไว้ใน AUTOEXEC.BAT และควรเป็นคำสั่งแรก ๆ

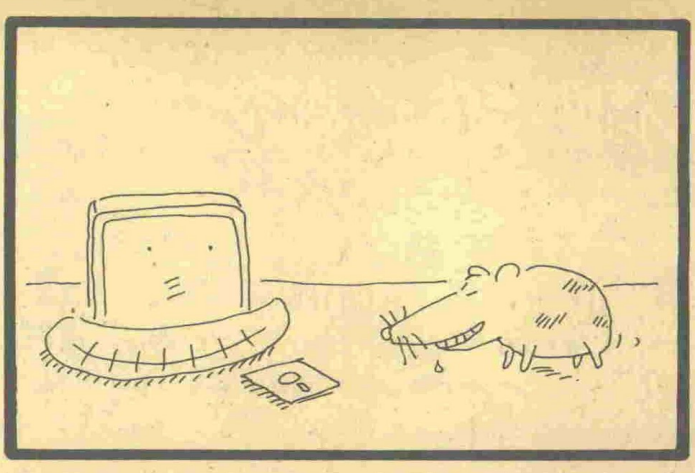
แต่บางทีอาจมีโปรแกรมไปถอนหรือห้ามไม่ให้ KILL ทำงาน ขอให้รัน PIG ทุกครั้งเมื่อจบการทำงานกับโปรแกรมหนึ่ง ๆ หากพบไวรัสล่ะก็ขอให้ปิดเครื่องและดำเนินการใหม่ดังจะกล่าวต่อไป

- หากคุณสงสัยว่าในฮาร์ดดิสค์หรือในดิสเกตต์มีไวรัสหรือไม่ ขอให้ใช้ PCTools หรือ Norton Utility ตรวจหาคำว่า sUMsDoS (โดยป้อนเป็น UMsDOS ก็พอ) คงจะต้องใช้เวลามากหน่อยครับสำหรับดิสเกตต์จำนวนมาก และเมื่อหาไม่พบจะให้ผมกล่าวว่ามั่นใจได้ 100% คงไม่ได้ เพราะอาจมีคนอุตริเปลี่ยนชื่อก็ได้ แต่ขอให้ถือว่าไม่มีไวรัสไว้ก่อน ดิสเกตต์แผ่นใดที่ปิด write protect ได้ ขอให้ปิดเสียด้วย ต่อเมื่อต้องการทำงานจึงใช้ PIG ทดสอบทีละโปรแกรมภายหลัง

- ต่อไปนี้หากคุณได้โปรแกรมใหม่มา ขอให้ใช้ PC Tools หรือ Norton Utility ตรวจสอบตามวิธีดังกล่าวก่อนที่จะเก็บไว้หรือโหลดลงฮาร์ดดิสค์ และเพื่อให้แน่ใจควรจะทดลองรันโปรแกรมเหล่านี้ทีละโปรแกรม แล้วทดสอบด้วย PIG (โดยไม่มี KILL ฝังตัวอยู่)

เมื่อพบไวรัส

ถ้าคุณพบไวรัสในระบบของคุณ ไม่ต้องตกใจครับ (เพราะถึงอย่างไรก็โดนแล้ว) หากคุณคิดว่ามีไวรัสฝังตัวอยู่ในหน่วยความจำ ทางที่ดีคือปิดเครื่อง แล้วบูต DOS ใหม่ด้วยแผ่นที่ปราศจากไวรัส



ในไดรฟ์ A จากนั้นค่อยรันโปรแกรม KILL ลองนึกทบทวนให้ดีว่าหลังจากรันโปรแกรม PIG ครั้งสุดท้ายจนพบไวรัสได้รันโปรแกรมใดไปบ้าง หรือตรวจสอบดิสค์ดังที่กล่าวมา ซึ่ง

- ถ้าอยู่ในดิสเกตต์ หากจำเป็นต้องเก็บไว้ ให้ใช้โปรแกรม PURE กำจัดไวรัส เมื่อดำเนินการเสร็จแล้วควรก๊อบปี้ไปไว้แผ่นใหม่แล้วฟอร์แมตดิสค์แผ่นเก่า

- ถ้าอยู่ในฮาร์ดดิสค์ ปกติแล้วควรจะมีโปรแกรมเหล่านี้เก็บไว้ในดิสเกตต์ ให้ลบไฟล์นั้นทิ้งไป แต่ถ้าจำเป็นต้องเก็บไว้ให้ก๊อบปี้ลงดิสเกตต์ แล้วจึงดำเนินการดังที่กล่าวมาข้างต้น ก่อนที่จะก๊อบปี้กลับไปยังฮาร์ดดิสค์ตามเดิม

แต่สำหรับที่หน่วยงานของผมปรากฏว่ามีไวรัสอยู่แทบทุกไฟล์ (.EXE กับ .COM) จึงต้องก๊อบปี้ไฟล์ข้อมูลลงดิสเกตต์แล้วฟอร์แมตฮาร์ดดิสค์ใหม่ (หากใช้ PURE กับฮาร์ดดิสค์โดยตรงจะกินเวลาหลายชั่วโมง)

การใช้ PIG

ในการใช้งาน PIG หลังจากคอมพายล์เป็นไฟล์ .EXE แล้ว ขอให้เก็บไฟล์ PIG.EXE ไว้ในไดเรคทอรีรองตัวใดก็ได้ตัวหนึ่ง แล้วก๊อบปี้มาไว้ที่ไดเรคทอรีหลักอีก 1 ตัว เพื่อสะดวกในการใช้ เมื่อ PIG พบไวรัส ตัวมันจะติดไวรัสด้วย ขอให้ลบทิ้งแล้วก๊อบปี้มาแทนที่

การใช้ PIG เมื่อรันโปรแกรม KILL แล้วเป็นเพียงมาตรการเสริมเพื่อให้มั่นใจเท่านั้น หากต้องการตรวจจับไวรัสโดยตรง คือเมื่อต้องการทดสอบไฟล์ใดไฟล์หนึ่งโดยเฉพาะจะต้องไม่รันโปรแกรม KILL ก่อน ไม่เช่นนั้นจะไม่มีประโยชน์อันใด เพราะไวรัสจะไม่ออกมาให้ PIG ทดสอบ ซึ่งเมื่อพบไวรัสจะต้องปิดเครื่องก่อนรันโปรแกรมอื่นใด รวมทั้ง PARK ด้วย

ยังไง ๆ ผมก็ขอให้คุณโชคดี แคล้วคลาดจากไวรัสทุกพันธุ์ เพราะไม่น่าสนุกเลยครับถ้าต้องเผชิญหน้ากับมัน